ferf
financial executives
research foundation

Sarbanes-Oxley Section 404 Compliance: From Project to Sustainability

Financial Executives Research Foundation (FERF) would like to acknowledge and thank FEI New York City Chapter for graciously underwriting the printing costs of this Executive Report.

ferf
financial executives
research foundation

the source for financial solutions

200 Campus Drive
P.O. Box 674
Florham Park, New Jersey 07932-0674
www.ferf.org

an affiliate of financial executives international

Sarbanes-Oxley Section 404 Compliance
From Project to Sustainability

William M. Sinnett
Director of Research
Financial Executives Research Foundation, Inc.

Dr. Robert A. Howell
Distinguished Visiting Professor of Business Administration
Tuck School of Business at Dartmouth

Sarbanes-Oxley Section 404 Compliance
From Project to Sustainability

TABLE OF CONTENTS

Sarbanes-Oxley Section 404 Compliance

From Project to Sustainability

Purpose

Although many aspects of the Sarbanes-Oxley Act of 2002 ("the Act") directly affect financial executives, members of Financial Executives International report that none have caused more additional effort and costs than Section 404 ("Section 404" or "404").

Section 404 requires management of public companies to include in their annual reports an assessment of the effectiveness of their internal controls over financial reporting. Compliance with Section 404 includes management's assessment of its controls, management's assertion whether these controls are effective, and an audit of these internal controls by the external auditor in conjunction with the audit of the financial statements.

While the effort to comply with Section 404 has provided some valuable insights, the time, redeployment of people, and other costs associated with the implementation in 2004 are generally viewed by members of Financial Executives International's (FEI's) Committee on Corporate Reporting (CCR) as not sustainable. Many financial executives from CCR member companies believe that evaluating the results and understanding leading practices of first-year implementation activities is an important step to the long-term sustainability of the Section 404 compliance process.

This report summarizes the compliance practices of leading companies during 2004, and it describes how they are improving their processes in the second year of compliance as they strive toward long-term sustainability. It is based on the experiences of the companies that participate on CCR.

Executive Summary

Based on their companies' experiences in complying with Section 404 of the Act, participants at a special CCR meeting identified and discussed the following compliance process improvements:

Key Controls

- Identify lower risk areas where reliance on the testing of company level controls is sufficient;
- Critically assess the necessary number of transaction-processing controls;
- Take some lower risk accounts out of scope;

- Reduce the number of testing locations with the use of shared service centers;
- Increase the number of and reliance on automated controls versus manual controls; and
- Find a balance between effective internal control and the number of key controls.

Risk Assessment

- Drive audit activity to the highest possible level in the organization;
- Take a top-down approach to risk and planning;
- Use risk assessment to help prioritize businesses and locations to get appropriate coverage;
- Integrate risk assessment with existing enterprise risk management (ERM) initiatives;
- Use shared service centers; and
- Consider the potential for fraud in assessing risk.

Segregation of Duties

- Ensure that all areas that represent key controls have established and sustainable segregation of processes;
- Use an automated software tool to test segregation of duties and system access;
- Prospectively test access with the software tool before actually assigning access; and
- Mitigate segregation of duties issues in small facilities.

System Implementations

- Evaluate risks associated with each system implementation; and
- Require self assessments from the process owners.

Management Testing of Controls

- Take a risk-based approach to testing;
- More testing should be done by management;
- Work with external auditors to develop credibility; and
- Reduce the use of external resources.

Evaluation of Results

- Take a risk-based approach to assessment and testing;
- Coordinate testing by management, internal audit, and external audit to identify deficiencies early and reduce their numbers;
- Use the whistleblower process to help identify potential deficiencies;
- Aggregate deficiencies across the organization to identify significant deficiencies;
- Use formal procedures and tools for tracking deficiencies; and
- Follow up on deficiencies identified in prior years.

Section 302 Certifications

- Use management self-assessment to support quarterly Section 302 representations; and
- Use software to streamline the certification process.

Auditor Issues

- Take a top-down approach to auditing to maximize efficiency;
- Work towards a greater reliance on internal audit's testing; and
- Negotiate the timing of external auditor testing to minimize the amount of roll-forward work.

Fostering Future Sustainability

For most companies, compliance with Section 404 of the Act was very costly in 2004, in terms of both time and expense. A March 2005 FEI survey of 217 companies found that employees of FEI member companies logged an average of over 26,000 hours per company during 2004 to comply with the regulations. In addition, member companies spent an average of $4.3 million for added internal staff time and additional fees for external auditors and other consultants. As described in this Executive Report, this time and expense was considered to be necessary to document, test, and audit thousands of individual transactions, so that companies could assert internal control over financial reporting.

During 2005, companies began to look for ways in which to work more efficiently in their compliance efforts. FEI arranged a special discussion session for Section 404 implementation leaders from some of the nation's largest companies, so that they could share their experiences with Section 404. Most participants agreed that the time and expense of compliance during 2004 was not sustainable, and that they would have to look for and implement process improvements.

Some of those process improvements are described in this Executive Report, and include:

- Use a top-down approach to risk and planning;
- Take low risk areas out of scope;
- Use risk assessment to get appropriate coverage;
- Require self-assessment from the process owners;
- Take a risk-based approach to testing;
- Use software to automate documentation, controls, and testing; and
- Work towards a greater reliance on management's testing by the external auditor.

As discussed by the participants, these approaches to Section 404 compliance were process improvements because they helped companies focus on those areas of the business that presented the greatest risk to financial misstatement. The participants agreed that their companies wanted to work more effectively and efficiently as they improved the control environments of their companies.

The May 16, 2005, Policy Statement issued by the Public Company Accounting Oversight Board (PCAOB) was often mentioned during the discussion session held on September 12, 2005. The participants agreed that the recommendations made in this policy statement should encourage closer cooperation between their companies and their external auditors as they looked for ways to more efficiently and effectively document, test, and audit their companies' internal controls.

Introduction

This Executive Report is based on a discussion by 38 Sarbanes-Oxley Section 404 implementation leaders from 33 of the nation's largest companies on their experiences with compliance with Section 404 during fiscal year 2004 and to date in 2005. The discussion session was held in Dallas, Texas, on September 12, 2005, in conjunction with a meeting of the Committee on Corporate Reporting (CCR), a national technical committee of Financial Executives International (FEI). FEI is a leading international organization of 15,000 members, including Chief Financial Officers, Controllers, Treasurers, Tax Executives, and other senior financial executives.

Members of CCR are primarily corporate controllers of Fortune 500 companies, and are responsible for their companies' financial reports.

The format for the one-day discussion session was based on a series of presentations by implementation leaders on the following aspects of Section 404 compliance:

- Key Controls,
- Risk Assessment,
- Segregation of Duties,
- Systems Implementations,
- Management Testing of Controls,
- Evaluation of Results,
- Section 302 Certifications, and
- Auditor Issues.

Implementation leaders made brief presentations on each of these aspects of compliance. Following each presentation, this report's co-author, Dr. Robert A. Howell, Distinguished Visiting Professor of Business Administration from the Tuck School of Business at Dartmouth, moderated a group discussion of other participants' related compliance experiences, and their plans for future compliance.

This Executive Report summarizes the participants' description of their companies' compliance practices during 2004 and to date in 2005, and describes their plans to improve their compliance processes for future sustainability.

Compliance process improvements are described qualitatively in this Executive Report, because the discussion session participants did not try to quantify the benefits to their companies for the other participants.

I. Key Controls

Process improvements for key controls include:

- Identify lower risk areas where reliance on the testing of company level controls is sufficient;
- Critically assess the necessary number of transaction-processing controls;
- Take some lower risk accounts out of scope;
- Reduce the number of testing locations with the use of shared service centers;
- Increase the number of and reliance on automated controls versus manual controls; and
- Find a balance between effective internal control and the number of key controls.

Compliance in 2004

Companies have established a hierarchy of internal controls
A standard hierarchy of controls would include:

- **Entity level controls:** High-level controls that usually support corporate governance, including codes of conduct and whistleblower procedures. Though these types of controls are included in risk assessments, they typically have a minimal effect on scope or transaction level testing. These controls can be used to mitigate other control deficiencies, but are the most difficult to tie to financial reporting.
- **Company level controls:** Mid-level controls for revenue and balance sheet accounts. These controls can be either preventive or detective.
- **Transaction controls:** Low-level controls governing individual transactions.

Most companies relied on too many key controls at the transaction level
Every key control must first be documented, then tested by management, and finally tested by the external auditor. Companies want at least 70% of their revenues and 70% of their balance sheets covered by key controls so that they can assert internal control over financial reporting.

Most companies decided that they had too many key controls at the transaction level in 2004, which then required them to do too much testing at a detailed process level.

Process Improvements for Sustainability

Identify lower risk areas where reliance on the testing of company level controls is sufficient
Routine transactions may be considered low risk and testing every transaction process can be time-consuming and costly. Look for company level controls

(higher than transaction controls) that will mitigate transaction level deficiencies and alleviate the necessity to test routine transactions.

Critically assess the necessary number of transaction-processing controls
Controls on many related transactions may be redundant. By evaluating the transactions and related controls, redundant controls can be combined or eliminated to achieve sufficient coverage.

Take some lower risk accounts out of scope
If an account is considered to have a remote risk of being materially misstated, it can be taken out of scope. The associated controls therefore do not need to be tested on an annual basis.

Reduce the number of testing locations with the use of shared service centers
Shared service centers centralize transaction processing, thereby reducing the number of individual locations where transactions need to be tested.

Increase the number of and reliance on automated controls versus manual controls
Automated controls foster a strong control environment.

Find a balance between effective internal control and the number of key controls
Reducing the number of key controls to be tested will reduce the annual cost of testing, but it may also reduce a company's internal control. Each company will have to find a balance between good internal control and a sufficient number of key controls. Many companies prefer to have some redundant controls, because they have decided that they are necessary for effective internal control.

II. Risk Assessment

Process improvements for risk assessment include:

- Drive audit activity to the highest possible level in the organization;
- Take a top-down approach to risk and planning;
- Use risk assessment to help prioritize businesses and locations to get appropriate coverage;
- Integrate risk assessment with existing ERM initiatives;
- Use shared service centers; and
- Consider the potential for fraud in assessing risk.

Compliance in 2004

Formal company-wide risk assessment is not widespread
Less than 50% of the participating companies did a comprehensive risk assessment during 2004.

External auditors have been risk-averse
The primary guidance for external auditors during 2004 was PCAOB Auditing Standard No. 2 (AS2), "An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements," issued by the PCAOB during the summer of 2004.

Many CCR member companies said that their external auditors applied AS2 in a rigid manner, and did not exercise judgment, so that their audits were detail oriented rather than cost-effective. They said that risk-averse auditors did not encourage a risk-oriented approach to internal control, forcing companies to document and test extensively at the transaction level. In other words, most companies took a "bottoms up" approach to documentation and testing during 2004.

The additional guidance issued by the PCAOB in May 2005 focused on a top down approach in identifying risk areas for internal control testing. However, the audit firms appear to be maintaining a conservative approach, waiting until they have had an opportunity to review the PCAOB's 2004 inspection reports before adjusting their audit approach to reflect this revised guidance.

Process Improvements for Sustainability

Drive audit activity to the highest possible level in the organization
In a top-down approach to internal control, there are fewer key controls at a company level compared to numerous detailed controls at the transaction level. Good internal control can be achieved by testing fewer controls at the company level. However, the company and its auditor should agree on where the risks reside in deciding at what level controls are tested.

Take a top-down approach to risk and planning

The guidance issued by the PCAOB in May 2005 encouraged external auditors to "use a top-down approach that begins with company-level controls, to identify for further testing only those accounts and processes that are, in fact, relevant to internal control over financial reporting, and use the risk assessment required by the standard to eliminate from further consideration those accounts that have only a remote likelihood of containing a material misstatement."

Use risk assessment to help prioritize businesses and locations to get appropriate coverage

In 2004, companies were striving to document and test as many income and balance sheet accounts as possible, because they were being encouraged by their external auditors to do so. Companies are now determining the optimal percentage of accounts that should be covered so that they can assert internal control over financial reporting.

There are a variety of approaches to get to an optimal coverage of revenue and balance sheet accounts. Some companies will focus on key locations in a geographic approach, and some will focus on their most significant financial accounts.

Regardless of the approach, the goal is to focus on those locations or accounts that present the most significant risk to financial misstatement. Some companies will decide to take entire locations out of scope, simply because they do not present a significant risk.

The risk assessment process may therefore reduce the number of physical locations and accounts that need to be included in the company's audit scope. If the risk assessment process thus reduces the number of locations and accounts to be included in scope, it can lead to a limited reduction in required documentation and testing.

CCR company participants generally believe that if their external auditors embrace this risk-based orientation to auditing, executives will be able to take a top-down, or risk-based, approach to internal control.

Integrate risk assessment with existing ERM initiatives

Companies with existing ERM initiatives have already identified potential risks and documented risk mitigation activities. They use these initiatives as a basis for determining what controls are necessary and need to be tested.

Use shared service centers
A shared service center concentrates more activity in one location. Companies can thus achieve greater coverage more efficiently by testing the processes at a shared service center. In addition, processes are controlled more effectively from a single location, which reduces the company's risk of financial misstatement.

Consider the potential for fraud in assessing risk
Fraud needs to be considered in the context of any risk assessment initiative.

Focus attention and testing on those businesses, locations, and transactions with the greatest potential for fraud. Conversely, transactions with less potential for fraud may be taken out of scope.

Leading companies have identified fraud risk factors and are currently reviewing these factors with their divisions. These fraud risk factors will receive special attention during the testing process.

III. Segregation of Duties

Process improvements for segregation of duties include:

- Ensure that all areas that represent key controls have established and sustainable segregation of processes;
- Use an automated software tool to test segregation of duties and system access;
- Prospectively test access with the software tool before actually assigning access; and
- Mitigate segregation of duties issues in small facilities.

Compliance in 2004

External auditors have segregation of duties templates
External auditors have provided some companies with segregation of duties templates for certain processes, such as the revenue cycle or the inventory cycle, so that the companies can check for segregation of duty deficiencies.

Companies have active segregation of duties monitoring programs
Companies track "movers" and "leavers" to monitor who has access to systems. Without an active segregation of duties monitoring program, segregation of duties tends to degrade over time. For example, systems users continue to request access, and more access requests are granted, but people change jobs. Specifically, if an employee had access to the accounts payable system in his old role, but should only be authorized to use the payroll system in his new job, is it a compliance breach to not revoke the accounts payable access once he had moved on to the new position?

Companies have identified segregation of duties security process issues
Companies have identified a number of security process issues related to segregation of duties:

- No defined data or process owners;
- Data/process owners may not understand security;
- Security team may not understand business risks;
- Data/process owners have different views on access;
- Users have different job responsibilities from location to location;
- Segregation of duties may not be a consideration in user and role maintenance; and
- Before the Sarbanes-Oxley Act of 2002, monitoring of segregation of duties was often limited to periodic audits.

Process Improvements for Sustainability

Ensure that all areas that represent key controls have established and sustainable segregation of processes.
Testing, mitigation, and remediation should be focused on key controls. Focus initially on key controls and then work with control owners to test a sample of transactions before finalizing a formal documentation template.

Use an automated software tool to test segregation of duties and system access
With an automated software tool, the user first specifies access rules and inputs a list of individuals, indicating levels of access requested for each individual. The software tool will then print a list of potential segregation violations based upon the rules specified. The user can either choose to remedy a violation by taking the offending access away from an individual, or can choose to mitigate that risk.

The tool does not fix problems, but does provide a detailed segregation analysis and identifies access problems. For best results, users should keep access rules as simple as possible, because segregation of duties can become very complex.

Here are the access rules suggested by one company:

Segregate these functions…	**…from these functions**
Create and change general ledger accounts and cost elements	Make journal entry postings to the general ledger
Setting pay rates Maintaining employee personnel records	Entering time data Cutting checks and/or direct deposit
Enter invoices Pay vendors	Purchasing Receiving
Vendor master maintenance	Enter invoices Pay vendors
Cash application	Sales order/credit memo entry Billing
Sales order/credit memo entry	Billing
Customer Master Maintenance (Accounting View)	Billing Delivery/Distribution Sales Order Entry Payment Processing

Prospectively test access with the software tool before actually assigning access
Software tool users can get a real time analysis of duty segregation by prospectively testing access before access is granted, to see if specific access creates any control issues.

Mitigate segregation of duties issues in small facilities

If a given location has a relatively small number of employees, some of those people may need to have access that would have otherwise been segregated in a larger facility. In these cases, potential segregation deficiencies can be mitigated by a division level review of balance sheet and income statement accounts.

IV. System Implementations

Process improvements for system implementations include:
- Evaluate risks associated with each[MG] system implementation; and
- Require self assessments from the process owners.

Compliance in 2004

Most companies did not permit new system implementations in the fourth quarter
In an informal survey of participating companies, two-thirds did not permit new system implementations in the fourth quarter of 2004.

Process Improvements for Sustainability

Evaluate risks associated with each system implementation
The Sarbanes-Oxley Program Office should evaluate the risks of a new (or modified) system implementation to Sarbanes-Oxley Section 404 assessment or Section 302 certification.

Sample questions to be considered in this evaluation could include:
- Are a number of implementations being planned for a given quarter? (This question addresses the managerial capabilities and capacity of the company's Information Technology [IT] department.)
- Will the system implementation be enterprise wide or just affect a specific location? (This question addresses the materiality of the implementation.)
- Will the system generate key financial information? (Smaller systems that aren't tied directly to the financial statements could be implemented up to fiscal year end.)
- How stable is the system? What are the system's testing results to date? (These question address the risk of bringing the system live.)
- Will the system be tested prior to quarter or year end? (Some companies will not implement a new system in the third month of a quarter, just as they will not implement in the fourth quarter of the year.)
- Are compensating procedures and controls in place? (This question addresses the possibility that the system will fail. Compensating controls are designed to catch errors in a new system.)

Require self assessments from the process owners
Self assessments should be completed by process owners during the development of the system, prior to going live, and immediately following going live. The process owners should do these assessments with assistance from the IT department. Some companies use formal checklists.

V. Management Testing of Controls

Process improvements for management testing of controls include:

- Take a risk-based approach to testing;
- More testing should be done by management;
- Work with external auditors to develop credibility; and
- Reduce the use of external resources.

Compliance in 2004

Most companies use self-assessment
Most companies use a self-assessment tool that is completed by the process owner or other management personnel.

Internal audit does the interim testing at most companies
While internal audit does the interim testing at most companies, the process owner or other management personnel does the testing at other companies. Some companies did continuous testing and others tested two or three times during the year in phases. In general, sample sizes were based on guidance from the external auditors.

There are different approaches to roll-forward testing
If interim testing was done earlier in the year, then roll-forward testing is required later in the year. Some companies used surveys, or simply asked management if anything had changed within their control environment. Other companies did limited testing and followed up on remediated items. Thus, a lot of testing was done in year one.

Process Improvements for Sustainability

Take a risk-based approach to testing
Use risk assessment to prioritize businesses and locations to test on an interim as well as annual basis.

More testing should be done by management
If more testing is done by management, including the process owners and their peer groups, internal audit's time will be freed up for their traditional operational audits and other special audits. Process owners should have the responsibility to do some of their own testing, to make sure that the controls are working as intended. Internal audit can then become more of a quality check.

Work with external auditors to develop credibility
Most companies spent an excessive amount of time and expense on compliance in 2004. For many companies, this time and expense paid off in well-documented internal controls, and the companies developed good credibility with their external auditors.

As external auditors place more reliance on the work of internal audit and the company’s control environment, they may be able to reduce the amount of their own testing that will be required.

Reduce the use of external resources
Companies used external resources extensively in 2004 as year one of compliance. These external resources included major auditing firms and other outside consultants.

Once processes are documented and controls are in place and tested, companies will be able to reduce their use of external resources, which are relatively expensive.

VI. Evaluation of Results

Process improvements for evaluation of results and deficiency assessment include:

- Take a risk-based approach to assessment and testing;
- Coordinate testing by management, internal audit, and external audit to identify deficiencies early and reduce their numbers;
- Use the whistleblower process to help identify potential deficiencies;
- Aggregate deficiencies across the organization to identify significant deficiencies;
- Use formal procedures and tools for tracking deficiencies; and
- Follow up on deficiencies identified in prior years.

Compliance in 2004

Companies used multiple sources to identify and evaluate deficiencies
Where work process owners are held responsible for internal control, self-assessment procedures helped identify deficiencies. If the process owner did not identify the deficiency, it was discovered by internal audit testing. Regardless of whether the deficiency was identified through self-assessment or internal audit testing, the work process owner was responsible for analyzing the results and defining an appropriate remediation plan.

Issues were individually prioritized based on magnitude and likelihood
In 2004, companies identified many deficiencies, and had to prioritize those deficiencies to be remediated. They were prioritized based on magnitude and likelihood, and companies focused on those deficiencies that represented the greatest risk to financial misstatement.

Companies were not very sophisticated in tracking deficiencies
Many companies used Excel spreadsheets or Access databases to track deficiencies. They documented the deficiency, the remediation plan, who was responsible for remediation, and the due date. However, this process had limited reporting and analysis capability.

Process Improvements for Sustainability

Take a risk-based approach to assessment and testing
When planning assessments and testing, give priority to those businesses, processes, accounts, and locations that present the greatest risks to the organization, and focus on key controls.

Coordinate testing by management, internal audit, and external audit to identify deficiencies early and reduce their numbers
Management and internal and external audit teams make long lists of processes with the greatest potential risk of deficiency. If these teams can work together to coordinate testing and compare lists earlier in the year, deficiencies can be identified, prioritized, and remediated sooner, rather than at year end. This will help avoid duplication of effort. The goal should be to achieve greater reliance on management testing by the external auditors.

Use the whistleblower process to help identify potential deficiencies
In addition to work process owner self-assessment and internal audit as sources of deficiencies, use the company's whistleblower process as a means to identify control deficiencies.

Aggregate deficiencies across the organization to identify significant deficiencies
Work process owners should be responsible for identifying and remediating deficiencies. However, as deficiencies are prioritized, management needs to monitor similar deficiencies across the organization that may be aggregated into significant deficiencies. Root causes of deficiencies should be addressed, and a formal escalation process should be established to ensure timely remediation.

Use formal procedures and tools for tracking deficiencies
Leading companies use special software solutions to track deficiencies. These integrated solutions have documentation, self-assessment, and remediation tracking and action plan functions, and will categorize deficiencies and link them to specific locations. They also provide enhanced monitoring, analysis, and reporting.

Follow up on deficiencies identified in prior years
Follow up on all outstanding issues identified in prior years. Even if they were minor, they may be symptoms of a weakened control environment, and could potentially be elevated into more significant deficiencies or even material weaknesses in future years

VII. Section 302 Certifications

Process improvements for Section 302 certifications include:

- Use management self-assessment to support quarterly Section 302 representations; and
- Use software to streamline the certification process.

Compliance in 2004

Companies continued their normal Section 302 quarterly certification processes
As mandated by Section 302 of the Act ("Section 302" or "302"), and formalized in a final rule issued by the Securities and Exchange Commission (SEC) in August 2002, companies have been providing CEO and CFO certifications of their annual and quarterly financial statements since 2002. As a basis for these certifications, companies developed in-house certification processes. These processes include sub-entity or divisional certification "roll-ups" and letters of representation.

Some companies have modified their existing 302 certification processes
In 2004, some companies made minor modifications to their 302 certification processes by adding additional language to the 302 certifications related to changes to internal control over financial reporting and increasing the number of management personnel required to complete 302 sub-certifications. Specifically, some leading companies have:

- Developed enhanced processes to identify material changes to internal control over financial reporting through improved questionnaires and checklists, including quarterly control certifications by entity management;
- Integrated 302 quarterly procedures and 404 controls documentation updates, including quarterly reporting of all changes to process documentation;
- Formally defined criteria to evaluate the materiality of changes to internal control over financial reporting; and
- Enhanced integration with information technology to help identify control changes that have occurred as a result of system implementation on a quarterly basis.

At these leading companies, quarterly processes have been formalized to support their 302 certifications and identify material changes to internal control over financial reporting. Groups responsible for identifying material changes to internal control over financial reporting varied, but generally included work process owners, a 404 project management office, management of operating units, and senior management.

Process Improvements for Sustainability

Use management self-assessment to support quarterly Section 302 representations

Some leading companies are not satisfied with their current certification process. They want sub-certifications to be based on self-assessments. In addition, they are conducting quarterly meetings to integrate the results of internal audit testing and management self-assessments to facilitate the analysis of material changes to internal control over financial reporting.

Use software to streamline the certification process

Some leading companies are implementing software to automate the certification process and facilitate the identification of changes to internal control over financial reporting. These companies are also investigating the potential to integrate this process with deficiency tracking software.

VIII. Auditor Issues

Process improvements for auditor issues include:
- Take a top-down approach to auditing to maximize efficiency;
- Work toward a greater reliance on internal audit's testing; and
- Negotiate the timing of external auditor testing to minimize the amount of roll-forward work.

Compliance in 2004

The external auditors tested all controls identified by management
According to most of the discussion session participants, both their companies and their external auditors decided that every process, even at a transaction level, had to be documented, and the related control had to be tested. As a result, in most cases, management identified numerous key controls, and the external auditors tested all of them in 2004.

Neither management nor external auditors used a risk-based approach to testing
When both the companies and their external auditors believed that all transactions, processes, and controls needed to be tested, management and the auditors effectively employed a "bottoms-up" approach to testing, and did not use a risk-based approach. In retrospect, this resulted in inefficiencies in both time and expense.

Reliance on management testing was limited
Because this was the first year in which to comply with new legislation and SEC rules, most external auditors were risk averse and decided to do all testing themselves.

The internal control audit was not integrated with the financial statement audit
Again, because this was the first year in which to comply with new legislation and SEC rules, most external auditors were risk averse. For most companies, the internal control audit was effectively a separate audit from the traditional financial statement audit.

Process Improvements for Sustainability

Take a top-down approach to auditing to maximize efficiency
Most companies agreed that they did not want to continue to pay their external auditors for as many hours worked and billed in 2005 as they did in 2004.

Leading companies are now looking for efficiencies in their external audit. They are now documenting higher level (company) controls, to be tested by both management and the external auditors, which should affect both the timing and extent of testing. A risk assessment of potential financial statement errors should affect the accounts identified as significant and amount of testing required.

Work toward a greater reliance on internal audit's testing
As management develops greater credibility with external auditors, and as the auditors become more comfortable with management's documentation and testing by internal audit, it is expected that the external auditors will place a greater reliance on management's monitoring and internal audit's testing of controls. As a result, the external auditors should be able to limit their work in low-risk areas, and put more focus on non-routine transactions and higher risk control areas.

Negotiate the timing of external auditor testing to minimize the amount of roll-forward work
All companies agree that roll-forward work should be minimized to make the audit as efficient as possible. How this will be done should be negotiated with the external auditor.

For example, some companies say that less risky areas should be audited early in the year, but not so early that they will have to be re-audited later in the year as part of the final audit. Likewise, higher risk areas should be audited early enough to remediate any deficiencies that are identified prior to year end. However, companies have to be careful not to schedule too much testing at year end, during the fourth quarter.

IX. Fostering Future Sustainability

For most companies, compliance with Section 404 of the Act was very costly in 2004, in terms of both time and expense. A March 2005 survey of 217 companies by Financial Executives International (FEI) found that employees of FEI member companies logged an average of over 26,000 hours per company during 2004 to comply with the regulations. In addition, member companies spent an average of $4.3 million for added internal staff time and additional fees for external auditors and other consultants. As described in this Executive Report, this time and expense was considered to be necessary to document, test, and audit thousands of individual transactions, so that companies could certify internal controls over financial reporting.

During 2005, companies began to look for ways in which to work more efficiently in their compliance efforts. FEI arranged a special discussion session for the Sarbanes-Oxley Section 404 implementation leaders from some of the nation's largest companies, so that they could share their experiences with compliance with Section 404. Most participants agreed that the time and expense of compliance during 2004 was not sustainable, and that they would have to look for and implement compliance process improvements.

Some of those process improvements were described in this Executive Report, and include:

- Use a top-down approach to risk and planning;
- Take low risk areas out of scope;
- Use risk assessment to get appropriate coverage;
- Require self-assessment from the process owners;
- Take a risk-based approach to testing;
- Use software to automate documentation, controls, and testing; and
- Work toward a greater reliance on management's testing by the external auditor.

As discussed by the participants, these approaches to Section 404 compliance were process improvements because they helped companies focus on those areas of the business that presented the greatest risk to financial misstatement. The participants agreed that their companies wanted to work more effectively and efficiently as they improved the control environments of their companies.

Many of these concepts can be found in the May 16, 2005, Policy Statement issued by the PCAOB. This policy statement "expresses the Board's view that to properly plan and perform an effective audit under Auditing Standard No. 2, auditors should -

- Integrate their audits of internal control with their audits of the client's financial statements, so that evidence gathered and tests conducted in the context of either audit contribute to completion of both audits;

- Exercise judgment to tailor their audit plans to the risks facing individual audit clients, instead of using standardized “checklists” that may not reflect an allocation of audit work weighted toward high-risk areas (and weighted against unnecessary audit focus in low-risk areas);
- Use a top-down approach that begins with company-level controls, to identify for further testing only those accounts and processes that are, in fact relevant to internal control over financial reporting, and use the risk assessment required by the standard to eliminate from further consideration those accounts that have only a remote likelihood of containing a material misstatement;
- Take advantage of the significant flexibility that the standard allows to use the work of others; and
- Engage in direct and timely communication with audit clients when those clients seek auditors’ views on accounting or internal control issues before those clients make their own decisions on such issues, implement internal control processes under consideration, or finalize financial reports.”

This PCAOB Policy Statement was mentioned often during the discussion session held on September 12, 2005. The discussion session participants agreed that these recommendations should encourage closer cooperation between their companies and their external auditors as they looked for ways to more efficiently and effectively document, test, and audit their companies’ internal controls.

Glossary

Account
An account is a record of debit and credit entries to cover transactions involving a particular item or a particular person or concern, or a statement of transactions during a fiscal period and the resulting balance. In the context of this report, account coverage represents the percentage of balance sheet and income statement account balances that are tested through 404 compliance procedures.

Auditing Standard No. 2
Auditing Standard No. 2, "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with An Audit of Financial Statements," (AS2) released by the Public Company Accounting Oversight Board (PCAOB) on March 9, 2004. AS2 provides examples of the different orders of magnitude of control deficiencies in its Appendix D. For example, not reconciling inter-company accounts is a control deficiency. Not having a formal process in place to ensure reconciliation would be considered to be a significant deficiency. If there are a significant number of material inter-company transactions, lack of a formal process would constitute a material weakness.

Control deficiency
A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. (AS2, Paragraph 8.)

Internal controls
Internal controls are the policies and procedures that a company must have in place to ensure that all its assets, liabilities, and transactions are properly reflected on its financial statements.

Material weakness
A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected. (AS2, Paragraph 10.)

Process
A process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, and performed by the company's board of directors, management, or other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:

(1) Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;

(2) Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and

(3) Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the company's assets that could have a material effect on the financial statements.

(From AS2, definition of “Internal Control over Financial Reporting,” paragraph 7. See also Securities Exchange Act Rules 13a-15(f) and 15d-15(f).2/)

Scope
The extent of treatment, activity, or influence.

Significant deficiency
A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the company’s ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that there is a more than a remote likelihood that a misstatement of the company’s annual or interim financial statements that is more than inconsequential will not be prevented or detected. (AS2, Paragraph 9.)

About the Authors

William M. Sinnett is Director of Research at Financial Executives Research Foundation, Inc. He received a Master of Business Administration from the University of Pittsburgh. Prior to joining FERF, he has held positions in financial management with Mellon Bank and Carnegie-Mellon University.

Dr. Robert A. Howell is Distinguished Visiting Professor of Business Administration at the Tuck School of Business at Dartmouth College. He received his Doctorate of Business Administration in Management Controls from Harvard University. He has combined a career as an academic, consultant, and executive across a broad spectrum of assignments to position himself as a leading authority on corporate governance and financial analysis, reporting, and control practices.

About Financial Executives Research Foundation, Inc.

Financial Executives Research Foundation, Inc. is the research affiliate of Financial Executives International. The purpose of the Foundation is to sponsor research and publish informative material in the field of business management, with particular emphasis on the practice of financial management and its evolving role in the management of business. The mission of the Research Foundation is to identify and develop timely, topical research to advance the financial management profession. The Foundation is an independent 501(c)(3) educational organization. The Foundation receives no portion of FEI Members dues; rather, it relies on voluntary tax-deductible contributions from corporations and individuals.

The views set forth in this publication are those of the author and do not necessarily represent those of the Financial Executives Research Foundation Board as a whole, individual trustees, employees, or the members of the Advisory Committee. Financial Executives Research Foundation shall be held harmless against any claims, demands, suits, damages, injuries, costs or expenses of any kind or nature whatsoever except such liabilities as may result solely from misconduct or improper performance by the Foundation or any of its representatives.

This and more than 80 other Research Foundation publications can be ordered by logging onto http://www.ferf.org

International Standard Book Number 1-933130-19-9

Printed in the United States of America

First Printing

Discussion Session Participants

Diane Allen
Global SOX Lead Manager
3M Company

Cindy Bond
Manager, Internal Controls
McCormick & Company, Incorporated

Tamara Candler
Associate Financial Consultant
Sarbanes-Oxley Coordinator
Eli Lilly and Company

Julie Caponi
Vice President, Audit
Alcoa Inc.

Colleen Cunningham
President and CEO
Financial Executives International

Jeff S. Dawson
Controller – SOX
Georgia-Pacific Corporation

Daniel A. DeRoma
Director, Internal Control Program Office
Eaton Corporation

Kamal Dua
Vice President & General Auditor
Comcast Corporation

Jim Eagen
Director, Professional Development
Financial Executives International

Randi Engelhardt
Director, Business Process Analysis
Cummins Inc.

Saul Gates
SOX Group Manager
Microsoft Corporation

Dr. Joachim Gebhard
Head of Corporate Financial Audit
Siemens AG

Linae Golla
Executive Director of Audit
Tenneco Automotive Inc.

Discussion Session Participants (continued)

Daniel Happer
Executive Director, External Financial Reporting
Time Warner Inc.

David Harris
Audit Manager
The Coca-Cola Company

Ellen M. Heffes
Executive Editor
Financial Executive Magazine
Financial Executives International

Jocelyn Henderson
Assistant Controller
The Washington Post Company

William Hogan
Senior VP, Finance
Computer Associates International, Inc.

Michael Holtman
Director
E.ON AG

Dr. Robert A. Howell
Distinguished Visiting Professor of Business Administration
Tuck School of Business
Dartmouth College

Michael Hultberg
Executive Director, Sarbanes-Oxley
Time Warner Inc.

Gregory A. Jamieson
SOX 404 Manager
The Coca-Cola Company

Nate Jenkins
Senior Financial Advisor
Exxon Mobil Corporation

Beth Karnes
Corporate Manager of Internal Controls
The Coca-Cola Company

Desmond Kealy
Sarbanes-Oxley Controls Manager
Intel Corporation

Anders Land
Chief Internal Control Officer
American International Group, Inc.

Brenda Lovcik
Finance Director
Medtronic, Inc.

Deborah Luening
Northrop Grumman Corporation

Juliana Maglathlin
Director, Financial Projects
Lockheed Martin Corporation

Martha Magurno
Director of Internal Control Compliance
The Dow Chemical Company

Barbara Maloney
Director SOX 404 Project
Motorola, Inc.

Jim Michaelson
Manager, Accounting Policy
Corning Incorporated

John Milliski
SOX 404 Process Leader
E.I. du Pont de Nemours and Company

Dwayne Milum
Director, External Reporting
Wal-Mart Stores, Inc.

Eugene Munson
SOX 404 Project Manager
The Procter & Gamble Company

Kelly Pasterick
Manager, SOX Compliance
Alcoa Inc.

Joseph Reitmeier
Director, Control Assessment
Cummins Inc.

Scott Samels
Manager of Internal Audit
McCormick & Company, Incorporated

Kevin Sierks
Manager, Finance
Guidant Corporation

William M. Sinnett
Director of Research
Financial Executives Research Foundation, Inc.

Discussion Session Participants (continued)

Anupam Tantri
Director, Business Controls
United Technologies Corporation

Steven Vivola
Vice President Finance & COO
J.P. Morgan Chase & Co.

Benjamin White
Director Internal Controls & Compliance
The Black & Decker Corporation

Financial Executives Research Foundation, Inc. would like to acknowledge the following for their support and generosity:

PRESIDENT'S CIRCLE DONORS

Abbott Laboratories, Inc.
ALCOA
AT&T
The Coca-Cola Company
Comcast Corp.
Corning Incorporated
Cummins, Inc.
CVS Corp.
Daimler Chrysler Corporation Fund
Dell Inc.
Dow Chemical Company
Duke Energy Corporation
E. I. du Pont de Nemours & Company
Eli Lilly & Company
Exxon Mobil Corporation
FEI Chicago Chapter
FEI Cincinnati Chapter
FEI Houston Chapter
FEI New York City Chapter
FEI Pittsburgh Chapter
FEI Silicon Valley Chapter
General Electric Company, Inc.
General Motors
Georgia-Pacific Corporation
Hewlett-Packard Company
IBM Corporation
Interpublic Group of Companies, Incorporated
Johnson & Johnson
Lockheed Martin Corporation
Microsoft Corporation
Medtronic, Inc.
Motorola, Inc.
Pfizer, Inc.
Procter & Gamble
Sony Corp. of America
Tenneco Automotive, Inc.
Verizon Foundation

ferf
financial executives
research foundation

business / research